Advances in Aerospace Cybersecurity

AIAA Space 2018

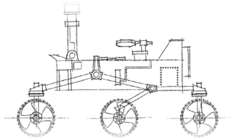
Jeremy Pecharich, Ph.D.
Cybersecurity Engineer
Cyber Defense
Engineering and Research, Group

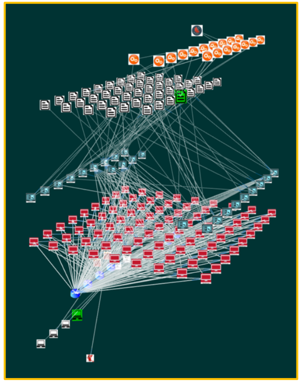
Jet Propulsion Laboratory
California Institute of Technology

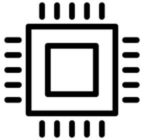
Cyber Defense Engineering and Research

Tasks and responsibilities, past and present

- Project/Program Office Cyber Defense Engineering
- Supports Cyber Security Improvement Project
- Non-NASA Reimbursable tasks (Power Grid, Oil and Gas, DoD)







- Fundamental research in Cyber Security
- Technology development
  - System Modeling and Analysis
  - Cyber/cyber-physical experiment test execution and validation
  - Hardware and software security technology transition to Industry
  - JPL Flight avionics with built-in security architectural provisions

“Oil Derrick” by Nikita Kozin, from thenounproject.com
“Transmission Tower” by Arthur Shlain, from thenounproject.com
“Processor” by Creative Stall, from thenounproject.com

Detecting Cyber Adversaries within Mission Environments

Analytics developed by the Sensor Mesh task, and piloted on M2020, provide visibility into anomalous behaviors that may indicate the "footprints" of cyber adversaries. Through the application of advanced machine learning-based sensors, missions will have the ability to detect more granular adversarial activity associated with stealthier threats.

Discovering Vulnerabilities – MIT Hackathon

MIT students participating in a "hackathon" worked with missions to identify weaknesses and correct flaws that would allow attackers access to mission systems. The hackathon was a successful event with great student participation, and resulted in the discovery of previously unknown vulnerabilities in mission software.

Cyber Analysis and Visualization Environment (CAVE)

Using modeling, analysis, and 3D visualization, CAVE enables a mission to assess its risks against cyber vulnerabilities. CAVE can be customized to the needs of each individual mission using visualization layouts, analysis plug-ins, and policy checking criterion. Europa Clipper is leveraging CAVE to perform cyber risk assessment.

Testing Mission Systems with Cyber Attacks

The JPL Cyber Testbed enables the resilience of flight project software and networks to be evaluated in the presence of adversarial activity. The testbed has been used to identify and analyze cyber security vulnerabilities in mission systems, e.g., the GDS for Jason 3, and to develop new detection capabilities.

Cybersecurity Capability Maturity Model

Developed JPL's Cybersecurity Capability Maturity Model (C2M2) based on the NIST Cybersecurity Framework. Mission-focused questions enable the assessment of a mission's security level.

Cyber Situational Awareness – Constellation Dashboard

Constellation assists mission GDS operators to rapidly identify and locate cyber anomalies in their ground systems, improving their ability to defend against adversarial incursions.

Defending Web Applications – Security Training

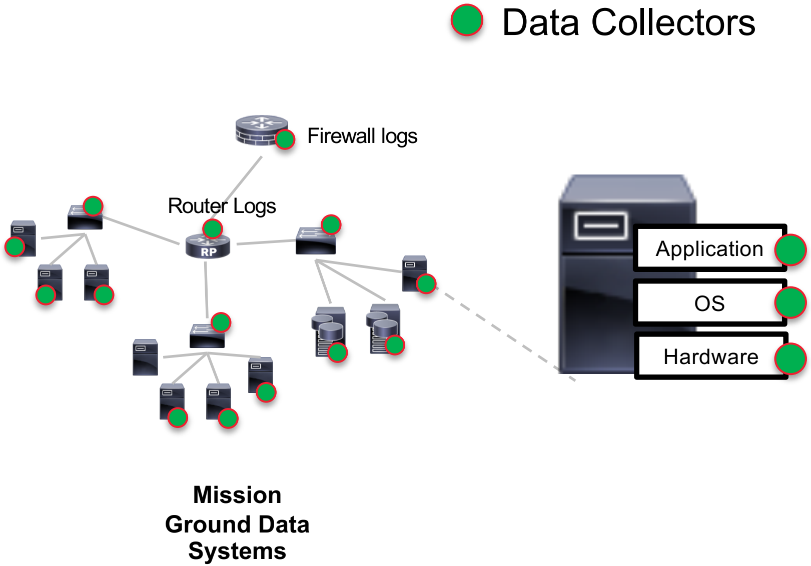
Mission web developers are formally trained to create web applications that are robust to cyber attacks. Developers are trained to defend against key cyber adversarial activities such as cross-site request forging, authentication bypass, and the exploitation of logic flaws.

Improving Mission Software Security

Evaluated and supported the deployment of security static code analyzers to detect and correct security vulnerabilities in core multi-mission software.

Sensor Mesh

Objective: Enhance mission cyber situational awareness



Data Collectors
(gather necessary cyber data from mission GDS)

- Combination of available tools and custom solutions.
- Developed a rigorous process to evaluate sensor performance impact within the Cyber Defense Lab (CDL)

Detectors
(detect anomalous behavior, and detect adversarial footsteps)

Correlation and Diagnostics
(correlate multiple ”anomalous signals”, reduce error, weed out false positives)

- Combination of simple and advanced (ML/AI) techniques to detect and diagnose anomalies and attacks.
- Analytics developed are rigorously evaluated within the Cyber Defense Lab.

Cyber Visualizations
(interface to the end-user, present relevant data to enhance situational awareness)

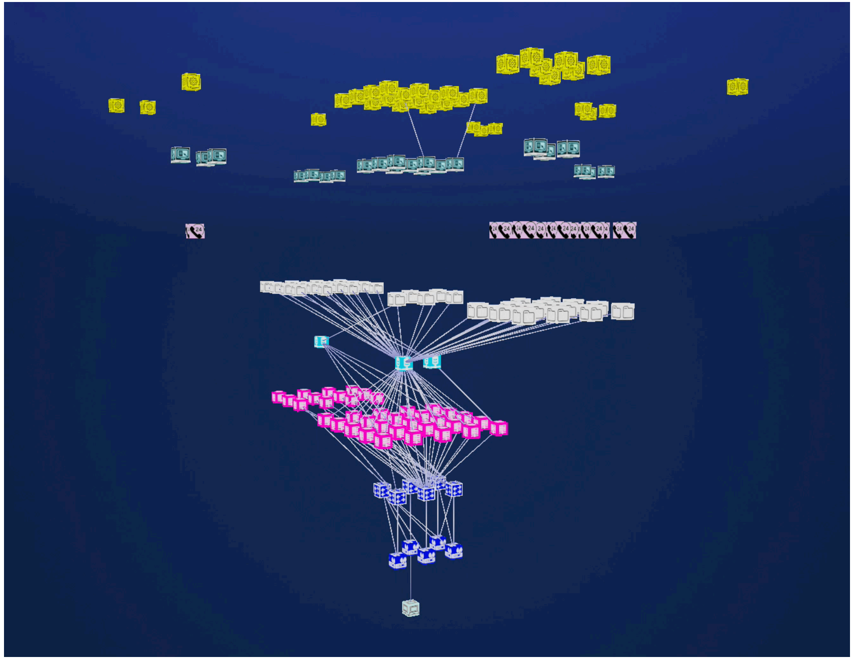
Working with the Human Centered Design group to explore novel visualizations to improve effectiveness of mission operators.

Cyber Defense Laboratory

- Project Cyber Validation & Verification
    - Project-specific verification of vulnerabilities, mitigation design, mitigation validation.
- Project Systems Simulation and Emulation
    - Ground systems.
    - Flight systems.
    - Communications.
    - CDL support services within an isolated environment.
        - AuthN, AuthZ, simulated DNS, Time, NAS storage, virtual and physical networking, virtual routing software with firewall capabilities, etc.
- Cyber-focused Research to support Projects
    - Modeling, analysis, detection, diagnosis, remediation.

Cyber Analysis and Visualization Environment (CAVE)

- JPL-developed, extensible, software framework to be used by the cyber analysts
- Model cyber-physical system
    - Hardware, software, files, connections, vulnerabilities , cost, risk
- Consequences of adversarial activities to mission objectives
- Report cyber-physical inventory to the mission
- Plug-in analysis architecture to run reasoning based analyses
    - For example, to determine if an adversary could traverse through the system to access a command file given system vulnerabilities and then deploy a mitigation strategy.
- Can track possible adversary entry/paths/goals given known weaknesses in our mission environment (i.e. CVEs, node centrality, proximity to the internet)
- Currently modeling mission in flight and development



Top Research Challenges in Aerospace Cybersecurity

- End-to-End encryption of sensitive data when one of your endpoints is on a “hostile” environment, i.e., Mars
- Applying COTS/Black Boxes to a mission critical environment when tolerance for error and resource error is very low
- Provenance and integrity of science and engineering data
- Performing cyber red team operations or even V&V on critical mission infrastructure

Jet Propulsion Laboratory
California Institute of Technology

jpl.nasa.gov